(19) JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: **11250568 A**

(43) Date of publication of application: **17 . 09 . 99**

(51) Int. Cl **G11B 20/10**

(21) Application number: **10045846**

(22) Date of filing: **26 . 02 . 98**

(71) Applicant: **SONY CORP**

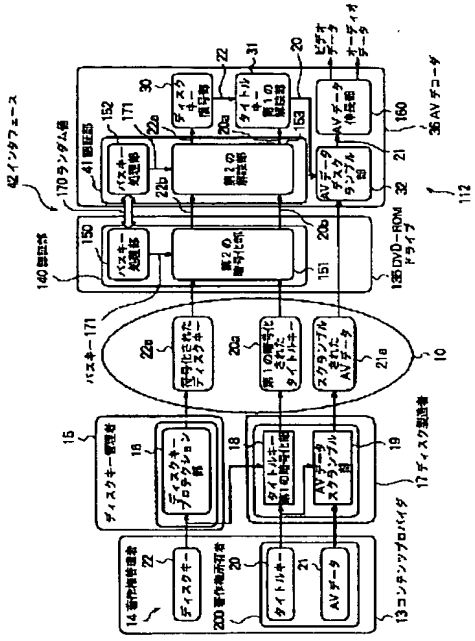
(72) Inventor: **MORI MASAHIRO**
NAKAMURA TADASHI

(54) READ-OUT DEVICE FOR RECORDING MEDIUM AND DATA PROCESSING DEVICE

(57) Abstract:

PROBLEM TO BE SOLVED: To provide a read-out device for an optical disk recording medium in which processing burden of a microcomputer can be lightened, in a DVD-ROM drive device.

SOLUTION: Key data 22a, 22b recorded in a DVD disk 10 and contents data 21a of which utilization is controlled by the key data are read out, read out key data 20a, 20b are ciphered by an authentication section 140, and the ciphered key data 20a, 20b and read out contents data 21a are transmitted to the outside through an interface 42. In the authentication section 140, data transfer accompanied by ciphering processing is controlled by a DMA section provided independently of the microcomputer performing servo control of rotation of the DVD disk and the like.



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平11－250568

(43)公開日　平成11年(1999)９月17日

(51)Int.Cl.[6]	識別記号	ＦＩ	
Ｇ１１Ｂ　20/10		Ｇ１１Ｂ　20/10	Ｈ

審査請求　未請求　請求項の数15　ＯＬ　（全９頁）

(21)出願番号　特願平10－45846

(22)出願日　平成10年(1998)２月26日

(71)出願人　000002185
ソニー株式会社
東京都品川区北品川６丁目７番35号

(72)発明者　森　雅弘
東京都品川区北品川６丁目７番35号　ソニー株式会社内

(72)発明者　中村　忠
東京都品川区北品川６丁目７番35号　ソニー株式会社内

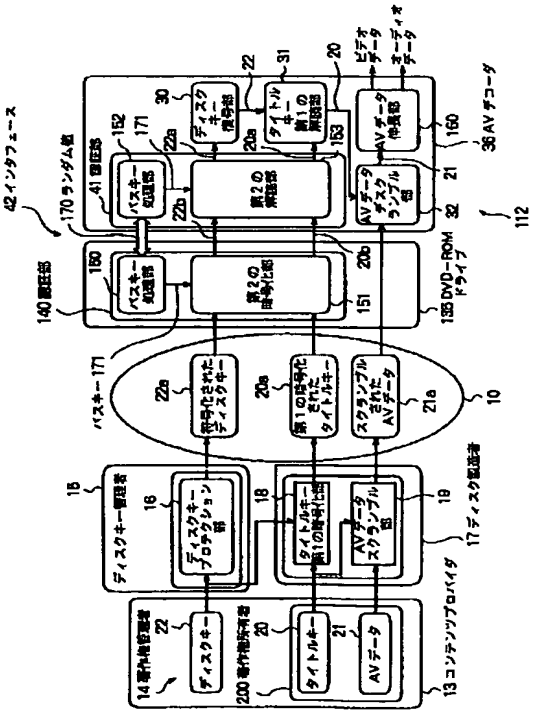
(74)代理人　弁理士　佐藤　隆久

(54)【発明の名称】　記録媒体読み出し装置およびデータ処理装置

(57)【要約】

【課題】　ＤＶＤ－ＲＯＭドライブ装置において、マイクロコンピュータの処理負担を軽減できる光ディスク記録媒体読み出し装置を提供する。

【解決手段】　ＤＶＤディスク１０に記録された鍵データ２２ａ，２０ａと当該鍵データによって利用が管理されるコンテンツデータ２１ａとを読み出し、読み出した鍵データ２０ａ，２２ｂを認証部１４０で暗号化し、当該暗号化された鍵データ２０ａ，２２ｂと読み出したコンテンツデータ２１ａとを、インタフェース４２を介して外部に伝送する。認証部１４０では、ＤＶＤディスクの回転などのサーボ制御を行うマイクロコンピュータとは別に設けられたＤＭＡ部によって、暗号化処理に伴うデータ転送が制御される。



1

【特許請求の範囲】

【請求項１】記録媒体に記録された鍵データと当該鍵データによって利用が管理されるコンテンツデータとを読み出し、前記読み出した鍵データを暗号化し、当該暗号化された鍵データを前記読み出したコンテンツデータと共に、インタフェースを介して外部に伝送する記録媒体読み出し装置において、

少なくとも前記記録媒体から前記鍵データおよび前記コンテンツデータを読み出す制御を含む、当該記録媒体読み出し装置における制御を統括的に行う第１の制御手段と、

前記読み出した鍵データおよび前記コンテンツデータを記憶する記憶手段と、

前記記憶手段に記憶された前記鍵データを暗号化する暗号化手段と、

前記記憶手段と前記暗号化手段との間の前記鍵データの転送を制御し、前記第１の制御手段とは別個に設けられた第２の制御手段とを有する記録媒体読み出し装置。

【請求項２】前記第１の制御手段、前記記憶手段、前記暗号化手段、前記第２の制御手段および前記インタフェースは、内部バスを介して接続してある請求項１に記載の記録媒体読み出し装置。

【請求項３】前記暗号化手段は、自らが生成したランダムデータと、前記インタフェースを介して入力したランダムデータとに基づいて、前記鍵データを暗号化する請求項１に記載の記録媒体読み出し装置。

【請求項４】前記第１の制御手段は、前記第２の制御手段に、暗号化処理の開始を指示する請求項１に記載の記録媒体読み出し装置。

【請求項５】前記第２の制御手段は、ダイレクトメモリアクセス方式を用いている請求項１に記載の記録媒体読み出し装置。

【請求項６】前記記録媒体は、光ディスク記録媒体である請求項１に記載の記録媒体読み出し装置。

【請求項７】前記コンテンツデータは、映像データである請求項１に記載の記録媒体読み出し装置。

【請求項８】前記コンテンツデータは、映像データおよび音響データである請求項１に記載の記録媒体読み出し装置。

【請求項９】記録媒体から読み出され、暗号化された鍵データと当該鍵データによって利用が管理されるコンテンツデータとを、インタフェースを介して、記録媒体読み出し装置からデコーダ装置に伝送するデータ処理装置において、

前記記録媒体読み出し装置は、

少なくとも前記記録媒体から前記鍵データおよび前記コンテンツデータを読み出す制御を含む、当該記録媒体読み出し装置における制御を統括的に行う第１の制御手段と、

前記読み出した鍵データおよび前記コンテンツデータを

2

記憶する記憶手段と、

自らが生成した第１のランダムデータと、前記インタフェースを介して前記デコーダ装置から入力した第２のランダムデータに基づいて、前記記憶手段に記憶された前記鍵データを暗号化する暗号化手段と、

前記記憶手段と前記暗号化手段との間の前記鍵データの転送を制御し、前記第１の制御手段とは別個に設けられた第２の制御手段とを有し、

前記デコーダ装置は、

前記インタフェースを介して前記記録媒体読み出し装置から入力した前記第１のランダムデータと、自らが生成した前記第２のランダムデータとに基づいて、前記インタフェースを介して入力した前記暗号化された鍵データを解読する解読手段と、

前記解読された鍵データを用いて、前記インタフェースを介して入力したコンテンツデータを利用可能にするコンテンツデータ処理手段とを有するデータ処理装置。

【請求項１０】前記記録媒体読み出し装置では、前記第１の制御手段、前記記憶手段、前記暗号化手段、前記第２の制御手段および前記インタフェースは、内部バスを介して接続してある請求項９に記載のデータ処理装置。

【請求項１１】前記第２の制御手段は、ダイレクトメモリアクセス方式を用いている請求項９に記載のデータ処理装置。

【請求項１２】前記記録媒体は、光ディスク記録媒体である請求項９に記載のデータ処理装置。

【請求項１３】前記コンテンツデータは、映像データである請求項９に記載のデータ処理装置。

【請求項１４】前記コンテンツデータは、映像データおよび音響データである請求項９に記載のデータ処理装置。

【請求項１５】前記第１の制御手段は、前記第２の制御手段に、暗号化処理の開始を指示する請求項９に記載のデータ処理装置。

【発明の詳細な説明】

【０００１】

【発明が属する技術分野】本発明は、ＤＶＤディスクなどの記録媒体に記録されたデータの読み出しを行う記録媒体読み出し装置およびデータ処理装置に関する。

【０００２】

【従来の技術】近年、ＤＶＤ(Digital Video Disc)プレーヤや、ＤＶＤ－ＲＯＭ(Read Only Memory)装置用のＬＳＩが活発に開発されている。ＤＶＤには、著作権保護の観点から、所定のアルゴリズムで符号化されたディスクキーと、暗号化(Encryption)されたタイトルキーとが記録されており、ＤＶＤプレーヤおよびコンピュータなどは、これら符号化されたディスクキーおよび暗号化されたタイトルキーを、それぞれ復号および解読しないと、記録されたＡＶデータ（コンテンツデータ）に利用できないようになっている。ここで、ディスクキーは、

例えば、１枚のＤＶＤディスクに１つ記録され、これを復号したときにのみ、ＤＶＤディスクに記録された他のデータの利用が許可される。また、タイトルキーは、ＤＶＤディスクに記録された複数のコンテンツのそれぞれに設けられ、復号されたタイトルキーに対応するコンテンツのＡＶデータのみ利用が許可される。

【０００３】図４は、ＤＶＤディスク１０へのディスクキーおよびタイトルキーの記録から、ＤＶＤディスク１０に記録されたＡＶデータをＤＶＤプレヤー１１およびコンピュータ（ＤＶＤ－ＲＯＭドライブ装置）１２を用いて再生するまでの過程を説明するための図である。図４に示すように、コンテンツプロバイダ１３の一人である著作権所有者２００が、著作権の対象となるＡＶデータ２１と、発行したタイトルキー２０とをディスク製造者１７に供給する。また、コンテンツプロバイダ１３の一人である著作権管理者１４が、ディスクキー２２を発行し、これをディスクキー管理者１５に供給する。ディスクキー管理者１５は、ディスクキープロテクション部１６において、ディスクキー２２を符号化する。この符号化されたディスクキー２２ａは、ＤＶＤディスク１０に記録される。

【０００４】ディスク製造者１７は、タイトルキー暗号化部１８でタイトルキー２０の第１の暗号化を行うと共に、ＡＶデータ２１をＡＶデータスクランブル部１９でタイトルキー２０を用いてスクランブル(Scramble)する。また、ディスク製造者１７は、第１の暗号化されたタイトルキーと、スクランブルされたＡＶデータと、ディスクキー管理者１５からの符号化されたディスクキー２２ａとを記録したＤＶＤディスク１０を製造する。

【０００５】ＤＶＤディスク１０は、出荷された後に、例えば、ユーザのＤＶＤプレーヤ１１にセットされる。ＤＶＤプレーヤ１１は、再生動作において、先ず、ディスクキー復号部３０で、符号化されたディスクキー２２ａを復号し、当該復号が成功すると、次に、当該復号されたディスクキーを用いて、ユーザから指示のあったコンテンツに対応するタイトルキーをタイトルキー解読部３１で解読し、当該解読に成功すると、次に、当該タイトルキーを用いて、対応するＡＶデータをデスクランブル部３２でデスクランブル(Descramble)して、ＡＶデータＳ１１としてディスプレイ３３に出力する。

【０００６】また、コンピュータ１２には、ＤＶＤ－ＲＯＭドライブ３５およびＡＶデコーダ３６が設けられている。ＤＶＤ－ＲＯＭドライブ３５とＡＶデコーダ３６とは、例えば、ＡＴＡＰＩ(AT Attachment Packet Interface)あるいはＳＣＳＩ(Small Computer System Interface)などのインタフェース４２を介して接続されている。ＤＶＤ－ＲＯＭドライブ３５には認証部(Authentication)４０が設けられている。ＤＶＤ－ＲＯＭドライブ３５では、インタフェース４２を介して伝送する鍵データに対して、認証部４０で所定の暗号化を行うことが、規格によって決められている。また、ＡＶデコーダ３６には、認証部４１、ディスクキー復号部３０、タイトルキー解読部３１およびＡＶデータデスクランブル部３２が設けられている。

【０００７】図５は、図４に示すＤＶＤ－ＲＯＭドライブ３５の構成図である。図５に示すように、ＤＶＤ－ＲＯＭドライブ３５は、データバス５５に、ＲＦ信号処理部５１、ＲＡＭ５２およびマイクロコンピュータ５３を接続した構成をしている。また、マイクロコンピュータ５３には、認証部４０が接続されている。データバス５５は、インタフェース４２に接続されている。

【０００８】以下、ＤＶＤディスクから読み出したＡＶデータを、インタフェース４２を介して、ＡＶデコーダ３６に出力する際のＤＶＤ－ＲＯＭドライブ３５の動作、いわゆるバス暗号化動作を説明する。図６は、この動作を説明するためのフローチャートである。先ず、マイクロコンピュータ５３からのサーボ制御に応じてＤＶＤディスクが回転し、光ピックアップ５０から、スクランブルされたＡＶデータ、第１の暗号化されたタイトルキーおよび符号化されたディスクキーが、ＲＦ信号処理部５１に出力される。これらのデータは、ＲＦ信号処理部５１において、波形整形などの処理が施された後に、データバス５５を介してＲＡＭ５２に記憶される（ステップＳ１）。そして、バス動作を開始前に、認証部４０において、自らが生成したランダムデータと、図４に示す認証部４１からインタフェース４２およびマイクロコンピュータ５３を介して入力したランダムデータとを用いてバスキーが生成される。認証部４０で生成されたランダムデータは、マイクロコンピュータ５３およびインタフェース４２を介して、認証部４１に出力される。そして、ＡＶデコーダ３６では、認証部４１が生成したランダムデータと、認証部４０から入力したランダムデータとを用いて、認証部４０で生成したものと同じバスキーが生成される。

【０００９】次に、タイトルの再生前に、ＲＡＭ５２に記憶された、第１の暗号化されたタイトルキーが、データバス５５を介して、マイクロコンピュータ５３に読み出される（ステップＳ２）。次に、マイクロコンピュータ５３に読み出された、第１の暗号化されたタイトルキーが認証部４０に出力される（ステップＳ３）。そして、認証部４０において、前述したように生成されたバスキーに基づいて、第１の暗号化されたタイトルキーが、さらに第２の暗号化される（ステップＳ４）。次に、第２の暗号化されたタイトルキーが、認証部４０からマイクロコンピュータ５３に読み出される（ステップＳ５）。次に、マイクロコンピュータ５３に読み出された、第２の暗号化されたタイトルキーが、データバス５５を介して、ＲＡＭ５２に書き戻される（ステップＳ６）。

【００１０】そして、ＲＡＭ５２に記憶された、スクラ

5

ンブルされたＡＶデータと、第２の暗号化されたタイトルキーが、データバス５５およびインタフェース４２を介して、図４に示すＡＶデコーダ３６に出力される（ステップＳ７）。次に、ＡＶデコーダ３６の認証部４１において、前述したバスキーを用いて、第２の暗号化されたタイトルキーが解読され、第１の暗号化されたタイトルキーが生成される。次に、既にディスク挿入時にディスクキー復号部３０で復号されたディスクキーを用いて、第１の暗号化されたタイトルキーがタイトルキー解読部３１で解読され、当該解読されたタイトルキーを用いて、スクランブルされたＡＶデータがデスクランブルされ、ＡＶデータが生成される。このＡＶデータは、例えば、伸長された後に、ディスプレイ３３に出力される。

【００１１】

【発明が解決しようとする課題】しかしながら、上述した従来のコンピュータ１２のＤＶＤ－ＲＯＭドライブ３５では、図６に示すように、ＲＡＭ５２から認証部４０への第１の暗号化されたタイトルキーの伝送（ステップＳ２，Ｓ３）、認証部４０からＲＡＭ５２への第２の暗号化されたタイトルキーの伝送（ステップＳ５，Ｓ６）や、ディスクキーの伝送が、マイクロコンピュータ５３を介して行われ、マイクロコンピュータ５３の処理負担が大きいという問題がある。すなわち、マイクロコンピュータ５３では、ＤＶＤ－ＲＯＭドライブ３５のサーボ制御の他に、ＤＶＤ－ＲＯＭドライブ３５における処理を統括的に制御するが、図６に示すステップＳ２，Ｓ３，Ｓ５，Ｓ６の処理などが行われる間は、他の制御が待たされてしまい、処理能力が低下するという問題もある。

【００１２】本発明は上述した従来技術の問題点に鑑みてなされ、ＤＶＤ－ＲＯＭドライブ装置において、マイクロコンピュータの処理負担を軽減できる記録媒体読み出し装置およびデータ処理装置を提供することを目的とする。

【００１３】

【課題を解決するための手段】上述した従来技術の問題点を解決し、上述した目的を達成するために、本発明の記録媒体読み出し装置は、記録媒体に記録された鍵データと当該鍵データによって利用が管理されるコンテンツデータとを読み出し、前記読み出した鍵データを暗号化し、当該暗号化された鍵データを前記読み出したコンテンツデータと共に、インタフェースを介して外部に伝送する記録媒体読み出し装置であって、少なくとも前記記録媒体から前記鍵データおよび前記コンテンツデータを読み出す制御を含む、当該記録媒体読み出し装置における制御を統括的に行う第１の制御手段と、前記読み出した鍵データおよび前記コンテンツデータを記憶する記憶手段と、前記記憶手段に記憶された前記鍵データを暗号化する暗号化手段と、前記記憶手段と前記暗号化手段との間の前記鍵データの転送を制御し、前記第１の制御手段とは別個に設けられた第２の制御手段とを有する。

6

【００１４】本発明の記録媒体読み出し装置では、第１の制御手段によるサーボ制御によって回転した記録媒体に記録された鍵データおよびコンテンツデータが第１の記憶手段に読み出される。また、例えば、前記第１の制御手段から第２の制御手段に暗号化処理の開始が指示され、第２の制御手段の制御に基づいて、前記記憶手段に記憶された鍵データが暗号化手段に出力され、当該鍵データが前記暗号化手段にて暗号化される。次に、前記暗号化された鍵データが、前記暗号化手段から前記記憶手段に転送されて記憶される。次に、前記記憶手段に記憶された、前記暗号化された鍵データが、インタフェースを介して外部に出力される。ここで、コンテンツデータは、例えば、ユーザに直接的に提供される画像データやアプリケーションプログラムなどである。

【００１５】また、本発明のデータ処理装置は、記録媒体から読み出され、暗号化された鍵データと当該鍵データによって利用が管理されるコンテンツデータとを、インタフェースを介して、記録媒体読み出し装置からデコーダ装置に伝送するデータ処理装置であって、前記記録媒体読み出し装置は、少なくとも前記記録媒体から前記鍵データおよび前記コンテンツデータを読み出す制御を含む、当該記録媒体読み出し装置における制御を統括的に行う第１の制御手段と、前記読み出した鍵データおよび前記コンテンツデータを記憶する記憶手段と、自らが生成した第１のランダムデータと、前記インタフェースを介して前記デコーダ装置から入力した第２のランダムデータに基づいて、前記記憶手段に記憶された前記鍵データを暗号化する暗号化手段と、前記記憶手段と前記暗号化手段との間の前記鍵データの転送を制御し、前記第１の制御手段とは別個に設けられた第２の制御手段とを有する。ここで、前記デコーダ装置は、前記インタフェースを介して前記記録媒体読み出し装置から入力した前記第１のランダムデータと、自らが生成した前記第２のランダムデータとに基づいて、前記インタフェースを介して入力した前記暗号化された鍵データを解読する解読手段と、前記解読された鍵データを用いて、前記インタフェースを介して入力したコンテンツデータを利用可能にするコンテンツデータ処理手段とを有する。

【００１６】

【発明の実施の形態】以下、本発明の実施形態に係わる記録媒体読み出し装置としてのＤＶＤ－ＲＯＭドライブについて説明する。図１は、本実施形態のＤＶＤ－ＲＯＭドライブ１３５が用いられるシステムの構成図である。図１において、図４と同じ符号を付したものは、前述したものと同じである。図１に示すように、コンテンツプロバイダ１３の一人である著作権所有者２００が、著作権の対象となるＡＶデータ２１と、発行したタイトルキー２０とをディスク製造者１７に供給する。また、

コンテンツプロバイダ１３の一人である著作権管理者１４が、ディスクキー２２を発行し、これをディスクキー管理者１５に供給する。ディスクキー管理者１５は、ディスクキー２２をディスク製造者１７のタイトルキー第１の暗号化部１８に供給すると共に、ディスクキープロテクション部１６において、ディスクキー２２を符号化する。この符号化したディスクキー２２ａは、ＤＶＤディスク１０に記録される。

【００１７】タイトルキー暗号化部１８は、ディスクキー２２を用いて、タイトルキー２０を第１の暗号化し、この第１の暗号化されたタイトルキー２０ａが、ＤＶＤディスク１０に記録される。また、ＡＶデータスクランブル部１９は、タイトルキー２０を用いて、ＡＶデータ２１をＡＶデータスクランブル部１９でスクランブル(Scramble)する。このスクランブルされたＡＶデータ２１ａは、ＤＶＤディスク１０に記録される。これにより、符号化されたディスクキー２２ａ、第１の暗号化されたタイトルキー２０ａおよびスクランブルされたＡＶデータ２１ａが記録された、ＤＶＤディスク１０が製造される。

【００１８】コンピュータ１１２は、本発明のデータ処理装置であり、ＤＶＤ－ＲＯＭドライブ１３５と、ＡＶデコーダ３６とを有する。ＤＶＤ－ＲＯＭドライブ１３５とＡＶデコーダ３６とは、ＡＴＡＰＩあるいはＳＣＳＩなどのインタフェース４２を介して接続されている。ＡＶデコーダ３６は、基本的に、前述した図４に示すものと同じである。

【００１９】ＤＶＤ－ＲＯＭドライブ１３５

ＤＶＤ－ＲＯＭドライブ１３５は、認証部１４０を有する。認証部１４０は、バスキー処理部１５０および第２の暗号化部１５１を有する。バスキー処理部１５０は、バス動作開始前に、自らが生成したランダムデータ１７２と、インタフェース４２を介してバスキー処理部１５２から入力したランダムデータ１７０とに基づいて、バスキー１７１を生成し、このバスキー１７１を第２の暗号化部１５１に出力する。

【００２０】第２の暗号化部１５１は、ＤＶＤディスク１０から読み出された符号化されたディスクキー２２ａを、ＤＶＤディスク１０の挿入時に、バスキー１７１を用いて第２の暗号化し、この第２の暗号化したディスクキー２２ｂを、インタフェース４２を介して、ＡＶデコーダ３６の第２の解読部１５３に出力する。また、第２の暗号化部１５１は、ＤＶＤディスク１０から読み出された第１の暗号化されたタイトルキー２０ａを、タイトルの再生時に、バスキー１７１を用いて第２の暗号化し、この第２の暗号化したタイトルキー２０ｂを、インタフェース４２を介して、ＡＶデコーダ３６の第２の解読部１５３に出力する。

【００２１】また、ＤＶＤ－ＲＯＭドライブ１３５は、ＤＶＤディスク１０から読み出した、スクランブルされたＡＶデータ２１ａを、インタフェース４２を介して、ＡＶデコーダ３６のＡＶデータデスクランブル部３２に出力する。

【００２２】ＡＶデコーダ３６

ＡＶデコーダ３６は、認証部４１、ディスクキー復号部３０、タイトルキー第１の解読部３１、ＡＶデータデスクランブル部３２およびＡＶデータ伸長部１６０を有する。

【００２３】認証部４１は、バスキー処理部１５２および第２の解読部１５３を有する。バスキー処理部１５２は、インタフェース４２を介して、ＤＶＤ－ＲＯＭドライブ１３５からＡＶデータ２１ａを入力する際に、図示しないランダム値発生器によってランダムデータ１７０を発生し、このランダムデータ１７０をインタフェース４２を介してバスキー処理部１５０に出力する。また、バスキー処理部１５２は、インタフェース４２を介してバスキー処理部１５０から入力したランダムデータ１７２と、ランダムデータ１７０とに基づいて、バスキー１７１を生成し、このバスキー１７１を第２の解読部１５３に出力する。このとき、バスキー処理部１５２が生成するバスキー１７１と、バスキー処理部１５０が生成するバスキー１７１とは同じである。

【００２４】第２の解読部１５３は、ＤＶＤディスク１０の挿入時に、インタフェース４２を介して入力した第２の暗号化されたディスクキー２２をバスキー１７１を用いて解読し、符号化されたディスクキー２２ａを生成する。第２の解読部１５３は、ディスクキー２２ａをディスクキー復号部３０に出力する。第２の解読部１５３は、タイトルの再生時に、インタフェース４２を介して入力した第２の暗号化されたタイトルキー２０ｂをバスキー１７１を用いて解読し、第１の暗号化されたタイトルキー２０ａを生成する。第２の解読部１５３は、タイトルキー２０ａをタイトルキー第１の解読部３１に出力する。

【００２５】ディスクキー復号部３０は、符号化されたディスクキー２２ａを復号してディスクキー２２を生成し、これをタイトルキー第１の解読部３１に出力する。タイトルキー第１の解読部３１は、ディスクキー２２を用いて、タイトルキー２０ａを解読してタイトルキー２０を生成し、これをＡＶデータデスクランブル部３２に出力する。ＡＶデータデスクランブル部３２は、インタフェース４２を介して入力した、スクランブルされたＡＶデータ２１ａを、タイトルキー２０を用いてデスクランブルしてＡＶデータ２１を生成し、これをＡＶデータ伸長部１６０に出力する。ＡＶデータ伸長部１６０は、圧縮されているＡＶデータ２１を伸長してＡＶデータを生成し、これをディスプレイに出力する。

【００２６】以下、ＤＶＤ－ＲＯＭドライブ１３５について詳細に説明する。図２は、ＤＶＤ－ＲＯＭドライブ１３５の構成図である。図２に示すように、ＤＶＤ－Ｒ

ＯＭドライブ１３５は、認証部１４０、光ピックアップ５０、ＲＦ信号処理部５１、ＲＡＭ５２、マイクロコンピュータ５３およびＤＭＡ(Direct Memory Access)部１９０を有する。図２において、図５と同じ符号を付した構成要素は、前述したものと同じである。図２に示すように、ＤＶＤ－ＲＯＭドライブ１３５は、データバス５５に、認証部１４０、ＲＦ信号処理部５１、ＲＡＭ５２およびＤＭＡ部１９０を接続した構成をしている。ＤＭＡ部１９０には、マイクロコンピュータ５３が接続されている。また、データバス５５は、インタフェース４２に接続されている。

【００２７】ＤＭＡ部１９０は、マイクロコンピュータ５３が関与しないＲＡＭ５２へのアクセスを実現し、具体的には、ＲＡＭ５２と認証部１４０との間でのデータ転送を実現する。以下、ＤＶＤディスク１０から読み出したＡＶデータを、インタフェース４２を介して、ＡＶデコーダ３６に出力する際のＤＶＤ－ＲＯＭドライブ１３５の動作を説明する。図３は、この動作を説明するためのフローチャートである。先ず、マイクロコンピュータ５３からのサーボ制御に応じてＤＶＤディスクが回転し、光ピックアップ５０から、スクランブルされたＡＶデータ２１ａ、第１の暗号化されたタイトルキー２０ａおよび符号化されたディスクキー２２ａが、ＲＦ信号処理部５１に出力される。これらのデータは、ＲＦ信号処理部５１において、波形整形などの処理が施された後に、データバス５５を介してＲＡＭ５２に記憶される（ステップＳ１１）。そして、バス動作を開始前に、認証部１４０において、自らが生成したランダムデータと、図１に示す認証部４１からインタフェース４２を介して入力したランダムデータとを用いてバスキーが生成される。認証部１４０で生成されたランダムデータは、インタフェース４２を介して、認証部４１に出力される。そして、ＡＶデコーダ３６では、認証部４１が生成したランダムデータと、認証部１４０から入力したランダムデータとを用いて、認証部１４０で生成したものと同じバスキーが生成される。

【００２８】また、マイクロコンピュータ５３から、ＤＭＡ部１９０にバス暗号化動作の開始が指示される（ステップＳ１２）。

【００２９】次に、タイトルの再生前に、ＤＭＡ部１９０による制御によって、ＲＡＭ５２に記憶された、第１の暗号化されたタイトルキー２０ａが、データバス５５を介して、認証部１４０に読み出される（ステップＳ１３）。次に、認証部１４０において、バスキー１７１に基づいて、第１の暗号化されたタイトルキー２０ａが、さらに第２の暗号化される（ステップＳ１４）。これによって、第２の暗号化されたタイトルキー２０ｂが生成される。

【００３０】次に、ＤＭＡ１９０による制御によって、第２の暗号化されたタイトルキー２０ｂが、データバス５５を介して、認証部１４０からＲＡＭ５２に読み出される（ステップＳ１５）。すなわち、ステップＳ１３～Ｓ１５の処理の制御は、マイクロコンピュータ５３ではなく、ＤＭＡ部１９０によって自動的に行われる。次に、ＲＡＭ５２に記憶された、スクランブルされたＡＶデータ２１ａおよび第２の暗号化されたタイトルキー２０ｂが、データバス５５およびインタフェース４２を介して、ＡＶデコーダ３６に出力される（ステップＳ１６）。

【００３１】そして、ＡＶデコーダ３６では、バスキー処理部１５２において前記バスキー１７１を用いて、第２の暗号化部１５１において、第２の暗号化されたタイトルキー２０ｂが解読され、第１の暗号化されたタイトルキー２０ａが生成される。この第１の暗号化されたタイトルキー２０ａはタイトルキー第１の解読部３１に出力される。

【００３２】タイトルキー第１の解読部３１では、ディスク挿入時に既に前述したタイトルキーと同様の過程を経てディスクキー復号部３０で復号されたディスクキー２２を用いて、第１の暗号化されたタイトルキー２０ａが解読され、当該解読されたタイトルキー２０がＡＶデータデスクランブル部３２に出力される。ＡＶデータデスクランブル部３２では、タイトルキー２０を用いて、スクランブルされたＡＶデータ２１ａがデスクランブルされ、ＡＶデータ２１が生成される。このＡＶデータ２１は、例えば、伸長された後に、ディスプレイ３３に出力される。

【００３３】以上説明したように、ＤＶＤ－ＲＯＭドライブ１３５によれば、ＲＡＭ５２と認証部１４０と間でのタイトルキーおよびディスクキーの転送を、マイクロコンピュータ５３による制御ではなく、ＤＭＡ部１９０による制御で実現する。そのため、マイクロコンピュータ５３は、図３に示すステップＳ１２において、ＤＭＡ部１９０にバス暗号化動作の開始を指示した後は、当該バス暗号化処理からは開放され、他の処理を行うことができ、マイクロコンピュータ５３の処理負担が軽減される。その結果、マイクロコンピュータ５３の処理が高速化される。

【００３４】本発明は上述した実施形態には限定されない。上述した実施形態では、記録媒体として、ＤＶＤディスクを例示したが、インタフェースを介して記録データを伝送するときに暗号化が要求される規格を持つものであれば特に限定されない。

【００３５】

【発明の効果】以上説明したように、本発明の記録媒体読み出し装置およびデータ処理装置によれば、第１の制御手段の処理の負担を軽減できる。

【図面の簡単な説明】

【図１】図１は、本発明の実施形態のＤＶＤ－ＲＯＭドライブ装置が用いられるシステムの構成図である。

【図２】図２は、図１に示すＤＶＤ－ＲＯＭドライブの構成図である。

【図３】図３は、ＤＶＤディスクから読み出したＡＶデータを、インタフェース４２を介して、ＡＶデコーダ３６に出力する際の図２に示すＤＶＤ－ＲＯＭドライブの動作のフローチャートである。

【図４】図４は、ＤＶＤディスクへのディスクキーおよびタイトルキーの記録から、ＤＶＤディスクに記録されたＡＶデータをＤＶＤプレヤーおよびコンピュータ（ＤＶＤ－ＲＯＭドライブ装置）を用いて再生するまでの過程を説明するための図である。

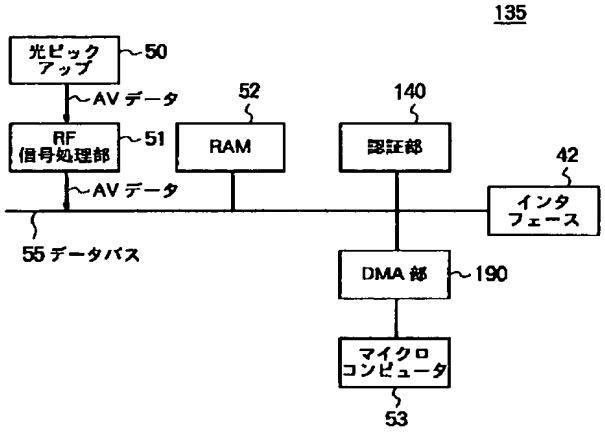
【図５】図５は、図４に示すＤＶＤ－ＲＯＭドライブの構成図である。

【図６】図６は、ＤＶＤディスクから読み出したＡＶデータを、インタフェース４２を介して、ＡＶデコーダ３＊６に出力する際の図５に示すＤＶＤ－ＲＯＭドライブの動作のフローチャートである。

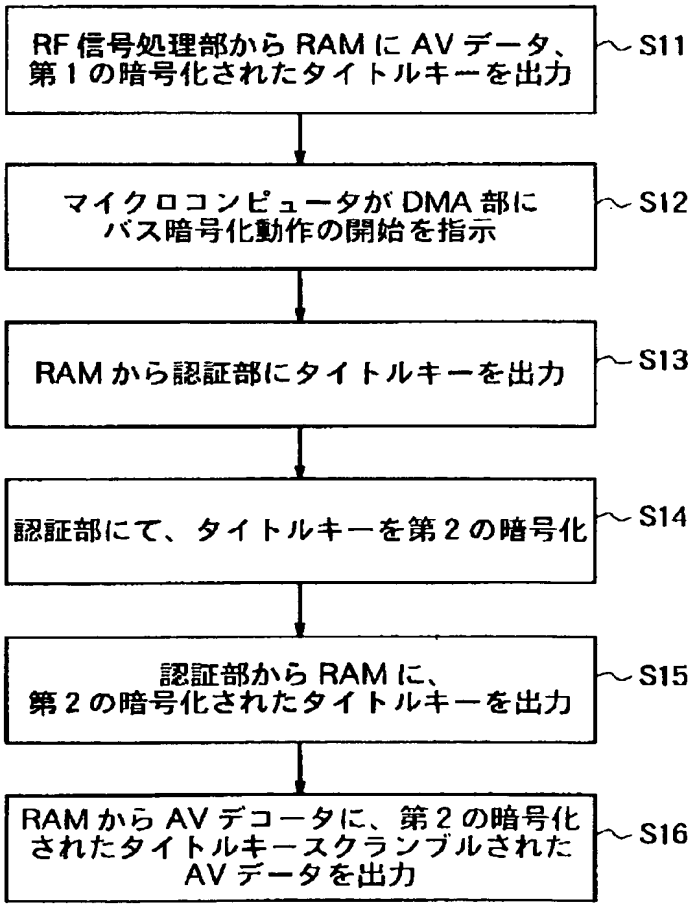
【符号の説明】

２０…タイトルキー、２０ａ…第１の暗号化されたタイトルキー、２０ｂ…第２の暗号化されたタイトルキー、２１…ＡＶデータ、２１ａ…スクランブルされたＡＶデータ、２２…ディスクキー、２２ａ…符号化されたディスクキー、２２ｂ…第２の暗号化されたディスクキー、３０…ディスクキー復号部、３１…タイトルキー第１の解読部、３２…ＡＶデータデスクランブル部、４０，４１，１４０…認証部、４２…インタフェース（ＡＴＡＰＩ）、５０…光ピックアップ、５１…ＲＦ信号処理部、５２…ＲＡＭ、１５０，１５２…バスキー処理部、１５１…第２の暗号化部、１５３…第２の解読部、１６０…ＡＶデータ伸長部、１９０…ＤＭＡ部

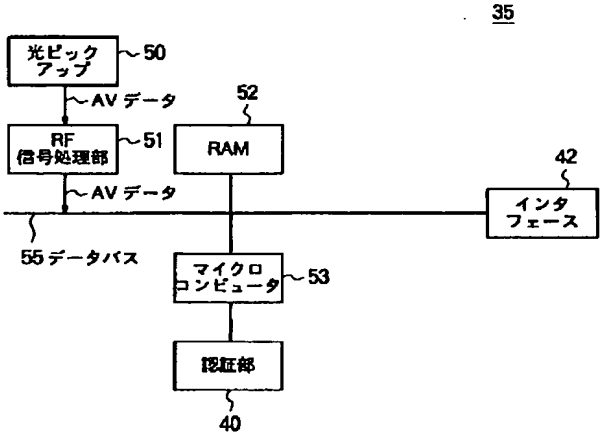
【図２】



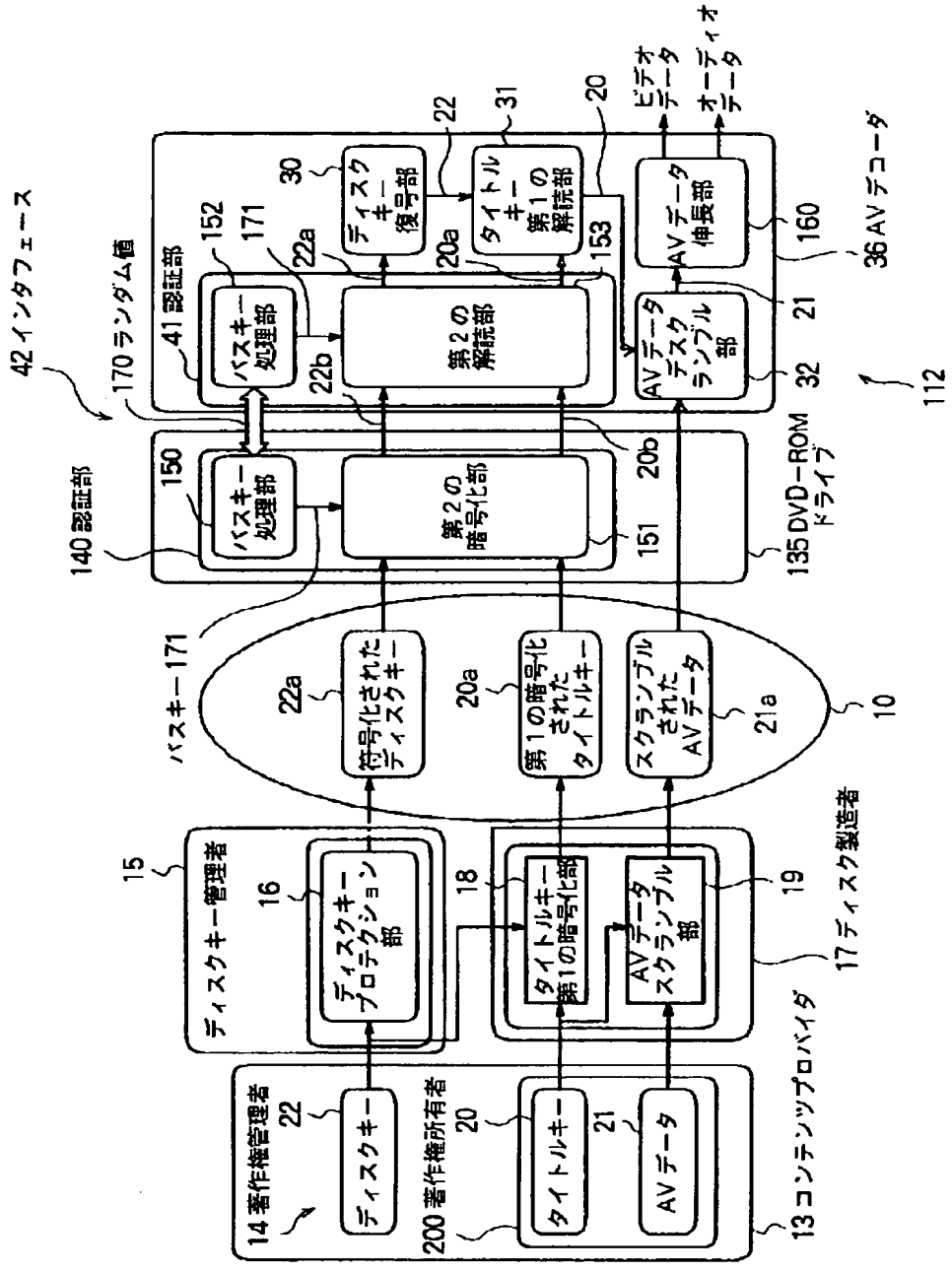
【図３】



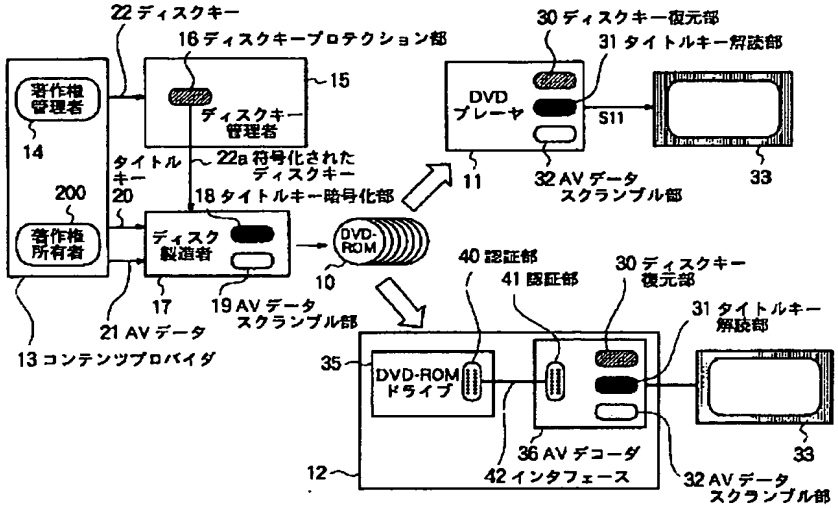
【図５】



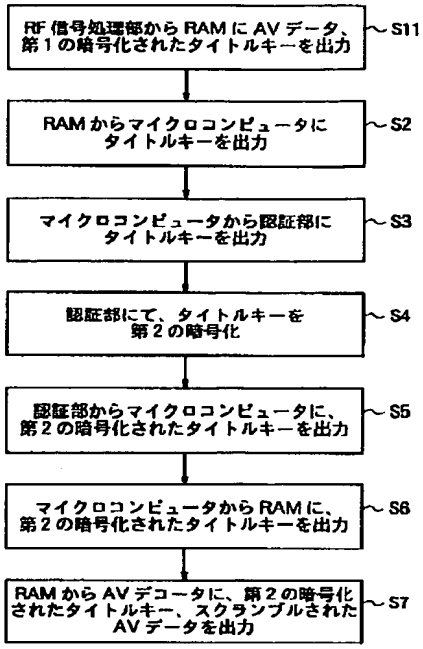
【図１】


42 インタフェース
170 ランダム値
41 認証部
152
171
30
22
31
20
ビデオデータ
オーディオデータ
ディスクキー復号部
タイトルキー第1の解読部
AVデータ伸長部
160
36 AVデコーダ
バスキー処理部
22a
20a
153
第2の解読部
AVデータデスクランブル部
21
32
112
140 認証部
150
バスキー処理部
22b
第2の暗号化部
151
20b
135 DVD-ROMドライブ
バスキー171
符号化されたディスクキー
第1の暗号化されたタイトルキー
スクランブルされたAVデータ
22a
20a
21a
10
15
ディスクキー管理者
16
ディスクキープロテクション部
18
タイトルキー第1の暗号化部
AVデータスクランブル部
19
17 ディスク製造者
14 著作権管理者
22
ディスクキー
200 著作権所有者
20
タイトルキー
21
AVデータ
13 コンテンツプロバイダ

【図４】


22 ディスクキー
16 ディスクキープロテクション部
30 ディスクキー復元部
31 タイトルキー解読部
著作権管理者
14
ディスクキー管理者
15
DVD プレーヤ
S11
タイトルキー
20
22a 符号化されたディスクキー
200
18 タイトルキー暗号化部
11
32 AV データスクランブル部
33
著作権所有者
ディスク製造者
DVD-ROM
10
40 認証部
41 認証部
30 ディスクキー復元部
31 タイトルキー解読部
17
19 AV データスクランブル部
21 AV データ
13 コンテンツプロバイダ
35
DVD-ROM ドライブ
36 AV デコーダ
42 インタフェース
12
32 AV データスクランブル部
33

【図６】


RF 信号処理部から RAM に AV データ、第１の暗号化されたタイトルキーを出力
S11
RAM からマイクロコンピュータにタイトルキーを出力
S2
マイクロコンピュータから認証部にタイトルキーを出力
S3
認証部にて、タイトルキーを第２の暗号化
S4
認証部からマイクロコンピュータに、第２の暗号化されたタイトルキーを出力
S5
マイクロコンピュータから RAM に、第２の暗号化されたタイトルキーを出力
S6
RAM から AV デコータに、第２の暗号化されたタイトルキー、スクランブルされた AV データを出力
S7